Notice of Allowability	Application No.	Applicant(s)	
	09/724,972	TRIMBERGER ET AL.	
	Examiner	Art Unit	
	Minh Dieu Nguyen	2137	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *June 5, 2006*.

2. ☒ The allowed claim(s) is/are *1-3,8-17,20-22 and 26-28*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☑ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

Allowable Subject Matter

1. This action is in response to the communication dated June 5, 2006 with the amendment to claims 1, 11 and 20-21 and the cancellation of claims 4-7, 18-19 and 23-25.

2. Claims 1-3, 8-17, 20-22 and 26-28 are allowed.

3. The following is an examiner's statement of reasons for allowance:

The present invention is directed to programmable logic device (PLD), more particularly to protection of designs loaded into a PLD through a bitstream. Efforts have been made to encrypt designs, but it is difficult to make the design both secure from attackers and easy to use by legitimate users. One mode of attack the design is if the PLD offers the option of reading back the bitstream after it has been loaded into the PLD, an attacker can read back this bitstream. Additionally, some PLDs offer the option of partial configuration (where several configuration addresses are specified for loading several portions of a design) and partial reconfiguration (where an existing design is not erased before new design data are loaded), an attacker could partially reconfigure a PLD to make successive portions of the design visible, and probably learn the whole design. To avoid such these attacks, the readback feature is disabled when encryption has been used and partial configuration and reconfiguration of PLDs loaded with encrypted designs are disallowed (i.e. "disabling readback of configuration data from the PLD after storing the configuration data in configuration memory; and disabling partial reconfiguration of the PLD in response to decryption of the configuration bitstream" in claims 11 and 20). Another mode of attack is to relocate portions of the encrypted

bitstream so that when they are unencrypted they are placed into visible portions of the PLD not intended by the designer. To prevent this relocation, address information is used in the encryption and decryption processes so that sending a portion of an encrypted bitstream to a different PLD location from that intended by the designer will cause it to decrypt differently into data with no meaning. Cipher block chaining (CBC) is used for achieving this result with the initial CBC value can be modified to incorporate the address of the data to force the decrypted data to be placed at a specific location in order to decrypt correctly (i.e. "wherein the decryption algorithm comprises the DES algorithm; and wherein the DES algorithm includes at least one cipher block algorithm selected from the group consisting of a cipher block chaining algorithm and a cipher feedback mode algorithm, and the address indicator is placed into a starter value of the at least one cipher block algorithm" in claims 1 and 21). The closest prior arts, Yip et al. (2001/0032318) and Kean (2001/0015919) fail to anticipate or render the above limitation obvious.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Minh Dieu Nguyen whose telephone number is 571-272-3873.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on 571-272-3865. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

mdn
6/14/06

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER